美国国家情报体系人工智能技术发展现状分析*

■ 黄敏聪
广东省科技图书馆（广东省科技信息与发展战略研究所） 广州 510070

摘要：［**目的/意义**］分析美国国家情报体系人工智能技术的实施背景及意义，并根据美国中央情报局及美国国防情报局等国家情报机构的人工智能项目实施内容、方向以及模式，归纳美国国家情报体系人工智能技术的发展趋势，从而提出对我国国家情报体系 AI 技术应用的启示。［**方法/过程**］利用文献调研法和比较分析法进行研究，分析 CIA 以及 DIA 等机构的人工智能项目实施内容，以及美国国家情报体系 AI 技术发展的优势。［**结果/结论**］从项目数量、支持资金以及发展规划看，美国国家情报体系正以难以想象的速度发展 AI 技术，特别是 In-Q-Tel 公司的推动成为关键因素。我国国家情报体系应该借鉴美国的先进经验，加快 AI 技术的部署与应用，特别是借助我国互联网企业的力量。

关键词： 美国 国家情报体系 人工智能
分类号： G20
DOI： 10.13266/j.issn.0252-3116.2018.11.015

1 研究背景、现状与方法

1.1 研究背景

人工智能（AI）技术的快速发展已经引起了全球关注，未来的 AI 技术有可能与核武器、飞机、计算机和生物技术一样，成为给国家安全带来深刻变化的颠覆性技术。AI 的每一种技术都为美国国家安全机构的战略、组织、优先事项和资源分配带来重大变革，其未来影响力至少可与核武器比肩。近年来，美国中央情报局（Central Intelligence Agency，CIA）、美国国防情报局（Defense Intelligence Agency，DIA）等政府机构都相继开展了大量运用 AI 技术的情报分析项目，试图将美国 AI 技术优势转变为国家战略情报优势，争取国家层面的最大利益。

2017 年 7 月，应美国情报高级研究计划局（Intelligence Advanced Research Projects Activity，IARPA）的要求，哈佛大学肯尼迪政治学院贝尔弗科学与国际事务中心发布了《人工智能与国家安全》（artificial intelligence and national security）报告[1]，将 AI 对美国国家安全的巨大影响列入当前影响美国国家安全的重要危险之一，分析了 AI 对于美国国家情报体系的重要影响，并为 AI 运用到国家情报体系设定了 3 个目标：①保持美国领先优势，为军事和情报能力优势提供砝码；②支持 AI 用于和平和商业用途的情报支撑，帮助民事和商业部门享受 AI 技术带来的好处；③运用 AI 技术提供的情报，减少灾难性风险，防范或降低偶发/敌对事件带来的严重后果。

1.2 研究现状

对 AI 技术研究的爆发期始于 2015 年，随着 ALPHA GO 软件的出现，全球开始了了对 AI 技术及其发展趋势的研究热潮。2017 年 7 月，美国情报高级研究计划局发布的《人工智能与国家安全》报告正式开启了国家情报与 AI 技术结合的研究，在国内外掀起了广泛关注，大量互联网网站（诸如腾讯、网易）等媒体大篇幅进行报道，并对其报告核心内容进行翻译。从调查数据以及信息看，美国对于 AI 技术与国家情报的结合早在 2000 年左右便开始进行，通过 CIA 下属的国家风险投资公司大规模对硅谷相关企业进行投资，并持续资助 10 余年，这使得美国 CIA 等国家情报机构掌握了 AI 技术与国家情报融合发展的技术制高点。

从我国研究现状看，根据 CNKI 等数据库检索结果（截至 2018 年 1 月 31 日），我国相关学者对 AI 技术

* 本文系广东省科学院引进高层次领军人才专项资金项目“技术与产业创新发展情报分析团队”（项目编号：2016GDASRC-0107）和广东省科学院科研平台环境与能力建设专项资金项目“技术与产业创新决策分析研究平台培育”（项目编号：2016GDASPT-0303）研究成果之一。
作者简介：黄敏聪（ORCID：0000-0002-5223-8462），粤创中心主任助理，馆员，E-mail：249053664@qq.com。
收稿日期：2017-12-08 修回日期：2018-01-31 本文起止页码：127-134 本文责任编辑：王传清

与国家情报体系建设结合的研究几乎是空白。这一方面是由于 AI 技术在 2015 年前后才呈现爆发趋势，另一方面是由于我国国家情报体系等相关体制机制尚未建立。2015 年，我国情报学界专家包昌火、张家年[2-3]等人先后发文建议我国应尽早建立国家情报体系架构，并以国防部、国家安全部以及公安部 3 个机构为骨干进行建设。由此可见，我国国家情报体系建设目前还远远落后于美国等国家。基于此，研究美国国家情报体系如何和 AI 技术有机结合能够弥补我国目前在该领域的研究空白，有利于我国国家情报体系相关机构建设，同时也为我国 AI 技术产业（产业竞争力仅次于美国）资源打通服务国家情报体系的通道提供决策支撑。

1.3 研究方法

鉴于 AI 技术对美国国家情报体系发展的重要影响，本研究通过对 CIA、DIA 等美国重要国家情报机构近年公布的投资项目、技术需求等信息进行收集、整理与分析，从而归纳目前美国国家情报体系 AI 技术的发展特点、趋势以及方向。同时，结合互联网等公开渠道的报告、发言以及评论等信息，归纳目前我国国家情报体系 AI 技术的应用现状，并根据上述分析结果，提出我国国家情报体系发展 AI 技术的启示与建议。

2 美国国家情报机构 AI 技术发展趋势分析

2.1 美国国家情报机构 AI 技术项目内容分析

近年来，美国中央情报局国家安全局、国家地理空间情报局、国防部长/联席参谋长办公室、国防情报局、联邦调查局、国家侦察办公室、国土安全部等政府机构陆续开展了 AI 情报项目的实施，其中 CIA 以及 DIA 的项目开展数量、规模以及资金支持量最为庞大。

2.1.1 CIA　自 1947 年 CIA 建立以来，互联网就受控于中情局，并一直是 CIA 的特别项目。计算机的出现更是强化了这一局面，然而这种看似更为现代的方法在收集数据上依然非常缓慢。最终，与能够收集数据的 AI 比较时，这些方法就十分落后了，因为传统方式只能用于检索少量的数据。为了推动 AI 运用在情报收集与分析上的运用，CIA 正同时进行 137 个不同的 AI 项目[4]，这些项目大部分通过“In-Q-Tel”（以下简称 IQT）公司进行筛选并进行资助，而 IQT 公司作为非营利组织，其高效地市场化手段为 CIA 的 AI 技术项目推进做出了突出的贡献。IQT 公司协助 CIA 近年推进的部分 AI 项目分析如表 1 所示：

表 1　In-Q-Tel 公司近年来推进的部分 AI 项目[4]

企业	地点	初始投资时间（年－月）	战略合作时间（年－月）	项目内容
Primer	旧金山	2016－06	2017－10	利用 AI 技术构建机器学习系统，可自动分析和汇总大量非结构化数据和自然语言文档
Metabiota	旧金山	2017－06	2017－08	利用 AI 技术，建立业界首个估计疫情防备和风险的情报分析平台。减少美国国家传染病爆发风险，并可衡量各国国家检测和应对疫情的能力
Ombud	丹佛	2016－12	2017－05	利用 AI 技术，应用于决策管理和知识协作，为政府机构、企业等提供高效决策管理平台
Algorithmia	西雅图	无	2016－07	利用该公司的 AI 算法接口，加速政府部门的应用平台以及管理系统等运用 AI 技术开发
Digital Immunity	马尔堡	2005－10	2016－06	利用该公司 Digital DNA Mapping 技术，使美国免受网络攻击，可防止几乎所有外来或恶意代码执行和利用任何漏洞，包括高级持续威胁（APT / AVT）及任何零日攻击
Brainspace	达拉斯	2016－06	—	利用该公司革命性处理信息方法，加速机器学习效率，进行超期案例评估及调查分析，并可对信息分类判别
Orbital Insight	帕洛阿尔托	2005－10	2016－06	利用卫星、无人机等地理空间图像数据，结合 AI 分析技术，预判区域或者全球社会经济发展趋势，例如监测全球石油供应能力，主要农产品供给，经济发展规模等
Databricks	旧金山	2015－03	2016－06	利用 AI 技术建立复杂分析领域开源数据处理引擎

基于敏感性，IQT 公司对外进行风投的企业、项目资金等都不是全部披露的，已经披露投资项目信息可查看其企业技术数据库（https://www.iqt.org/portfolio/）。根据上述企业技术数据库信息[5]，CIA 支持 AI 技术项目具体表现为以下特点：

（1）将 AI 技术覆盖数据产业全链条。从 CIA 支持的 AI 技术项目看，主要分为以下三大类，基本实现了对数据产业全链条的覆盖。①数据监测与产生（上游）。例如对空间地理数据与经济数据的特征抽取，加快数据生成的数据与质量（Orbital Insight 等企业）。②数据智能分析处理（中游）。例如开发智能数据分析引擎与自然语言数据处理平台等（Primer 等企业）。③数据应用与决策（下游）。例如对传染病与经济危机等重大国家事件的预测、处理等（Metabiota 等企业）。

（2）着重云端平台的运用。2016 年开始，CIA 加大了对 AI 技术云端平台使用的项目支持数量，诸如对

FRAME 等智能多系统云端平台。这是 CIA 作为美国国家情报体系的重要技术策动源,肩负了向美国其他国家情报机构扩散技术的使命。因此,云端平台的跨地域、跨机构以及跨系统特性,使得 AI 技术能够在不同情报机构之间快速实现应用。据 CIA 预测,未来美国国家情报体系的协同合作体系将高度依赖云平台实现。

(3)AI 技术的预判与优先支持。虽然 AI 技术成为热点是近两年才开始,但是 CIA 对于 AI 技术的投资可追溯到 2000 年前后。从 IQT 公司投资的项目可见,早在 2005 年,其已经对 Orbital Insight、Digital Immunity 公司进行了战略性投资。这些公司对 AI 技术的研究持续了 10 年以上,积累了扎实的技术基础。

2.1.2 DIA DIA 在其研究报告中指出,过去的几十年里,美国都是以一种缓慢而繁琐的方式支出防御资金。这种方式只允许谨慎地开发新项目,比如一艘航空母舰,它的设计可以持续几十年。这种模式显然无法跟上伊斯兰极端分子利用社交媒体进行恐怖活动的速度。因此,DIA 从 2015 年开始,启动了"创新完成计划"(DIA innovation implementation plan)[6],并通过其新的创新中心办公室来推动计划实施。在计划中,DIA 尝试运用 AI 技术,并结合企业以及外部技术项目,推动 DIA 在 AI 情报项目上的巨大飞跃。目前,每个被 DIA 创新计划支持的项目都能得到 25 万美元的种子资金,从而为 DIA 开发项目或者进行技术评估。2016 年,DIA 已经累计为 6 个 AI 项目投入了超过 200 万美元,资金来源自与国防创新实验小组(Defense Innovation Unit Experimental,DIUx)合作的一项专用预算[7]。目前,DIA 已经在 https://www.fbo.gov 和 https://www.grants.gov 两个网站建立了定期 AI 技术需求,社会各类组织可以随时进行项目方案申请,并获得资助。目前,DIA 在 AI 技术情报项目上主要有 18 个大需求方向[6],其主要内容如表 2 所示:

表 2 DIA 在 AI 技术情报项目上的 18 个大需求方向[8]

	方向	主要内容
1	机器学习和自然语言处理(Natural Language Processing,NLP)识别和组织大数据中的武器系统信息	DIA 力求了解利用机器学习技术与其他工具(如 NLP)结合使用的功能和方法,以自动识别与埋在各种数据源中的武器系统的复杂描述相关的技术术语和名称。这些数据源可能包括原始传感器文件,非结构化电子文档和各种类型的多媒体文件。这些文件也可能有各种格式。某些文件类型可能需要其他预处理工具,如光学字符识别及 NLP。一旦组织的专业知识被提炼成支持 AI 工具的知识系统,这些知识系统须能够被用来支持其他 AI 工具
2	AI 和机器学习工具进行收集、研究、信息监测、自动报告、专题数据管理、数据转换和数据库开发	DIA 寻求简化和加速某些情报工作流程的工具;压缩情报生产时间;整合多个数据集和格式;识别数据之间的关系;处理数据并辨别某个特定主题的相关性;促进信息共享;并为预测分析准备数据。工具须以各种格式处理大量非结构化数据,并可能适应动态数据流。AI 和机器学习还将支持精简和加速分析非结构化信息、音频、图像/可视化和视频的耗时/密集任务;了解将 AI 和机器学习应用于专题数据管理和数据转换能力
3	机器学习支持工作流程自动化	DIA 旨在了解使用机器学习工具自动化智能生产,计划和处理工作流程的功能和方法,以减少手动完成这些任务所花费的时间
4	预测分析、警报、指示和警告的工具(Instructions & Warning,I&W)	DIA 旨在了解在大数据框架内将 AI、机器学习和预测分析算法应用于指示和警告(I&W)的功能和方法。这种需求将确定可以对开源数据、情报传感器数据、产品智能、金融智能和其他形式的情报报告进行分析的半自动化工具,以定位趋势,创建需要关注的警报。解决方案将识别建模技术,并将分析和直观显示在平时和冲突期间在战场和控制区域观察到的变化的预测分析
5	利用 AI 的半自主多传感器融合	DIA 旨在了解有关技术的能力和方法,这些技术可利用支持 AI 的传感器处理器来管理和融合多个相同或不同现象的传感器,然后按类型识别和响应来源,并识别异常情况。AI 支持的传感器网络将根据感官馈源预测和响应已识别的威胁类型和威胁活动。感官馈源可包含来自声学、地震、磁场、密度/压力、电磁、无线电频率、电光/红外,高光谱和其他在空间和时间上的模拟和数字馈源
6	AI 和机器学习支持军事行动	DIA 旨在了解将多智能体传感器数据融合到战场,作战和战术层面的实时战场意识和预测分析的目标领域
7	AI 和机器学习支持业务运营	DIA 力求了解将 AI 和机器学习应用于商业领域的能力,包括收购管理、财务分析、投资组合的优先次序和优化、商业分析、风险管理、资源节约和商业决策支持。期望的解决方案将增强通过对军事业务财务运营的预测分析简化和获得洞察力的能力
8	AI 和机器学习支持数据科学环境	DIA 旨在了解将数据科学环境的目标领域应用 AI 和机器学习的行业能力。以确定支持和简化文本和音频数据的自然语言处理,推荐引擎、净流量数据和数据科学环境的功能
9	完成智能产品和知识管理的 AI 和机器学习支持	扫描所有已完成的情报产品,并从中创建一个有组织的知识体系,人们可用它来探索主题和概念。知识主体应该向用户返回一个答案,描述用户输入信息请求时数据之间的连接。该方案应返回重复的和冲突的数据源,为分析人员提供精确的全面的最终产品
10	AI 和机器学习支持开源信息采集	DIA 旨在了解使用 AI 和机器学习工具半自主地收集所有形式的开源信息,然后更新数据挖掘和发现分析技术的能力。解决方案应包括组合,比较和分析分类和开源资料的能力,并试图交叉验证从不同来源获得的信息
11	机器学习支持多任务管理	DIA 旨在了解将机器学习技术应用于处理来自多个来源(尤其是电子邮件)的传入任务的目标区域的功能。技术有助于确保管理人员追踪和捕获临时需求。该解决方案将利用机器学习工具读取电子邮件消息流,以发现、跟踪任务并将其路由到官方任务通道

（续表 2）

	方向	主要内容
12	AI 和机器学习支持动态威胁分析建模	DIA 旨在了解将动态威胁分析建模的目标领域应用 AI 和机器学习的能力。解决方案将形成一个自动化系统，允许分析人员利用量化的对手能力（使用分析人员的输入或从现有数据库中提取）、学说、影响、历史行为和陈述的意图来开发加权分析威胁模型
13	AI 和机器学习对绩效评估的支持	DIA 旨在了解将 AI 和机器学习应用于评估组织绩效评估的目标领域的行业能力。解决方案将在国防情报企业（DIE）中开发通用的性能测量功能，以支持 CCMD 和机构的优先级
14	AI 和机器学习支持人力资源招聘	解决方案将能够将结构化和非结构化数据源相关联，以便通过利用个人传记、专业知识档案和可用的在线数据来识别、推荐和排列任务最优军事人选组合
15	AI 和机器学习支持出版作者关系	DIA 旨在了解将 AI 和机器学习应用于评估出版物中所包含的结构化和非结构化数据的目标领域的能力，以显示作者之间关于特定主题的关系。解决方案应该利用自然语言处理，根据作者、合著者、机构、主题和其他细节之间的关系自动标记和构建网络
16	AI 和机器学习支持签名识别	DIA 旨在了解将人工智能和机器学习应用于识别来自各种传感器来源的目标的能力，以帮助开发、分析和生产。签名标识技术将支持弹道导弹技术收集，核监测和 MASINT 分析
17	AI 和机器学习支持记录管理	DIA 旨在了解将 AI 和机器学习应用于记录、业务分析和可视化前端和后端管理目标领域的能力。确定利用机器学习来管理、跟踪、分析趋势和预测员工职业发展机会的人才管理（人事）系统
18	AI 和机器学习支持网络安全	DIA 致力于理解将人工智能和机器学习应用于网络安全目标领域的行业能力。解决方案将有能力动态检测异常/风险/威胁。解决方案将比传统方案（基于数据收集、处理与分析模式）具有更快的分析速度以及数据处理规模。

DIA 支持的 AI 技术项目比 CIA 更为敏感，一般不对外公布项目投资企业、资金以及内容，但从以上其支持的项目方向以及公开信息看，其主要表现为以下特点：

（1）自然语言处理识别成为 AI 技术运用的重要方向。从 18 个方向的内容看，涉及 NLP 的 AI 技术应用有 4 个方向，NLP 应用得到了美国军事情报部门的高度重视。这一方面与 DIA 越来越注重社交媒体等数据采集有关，另一方面也与美国军事力量在全球部署息息相关。AI 技术在 NLP 中的应用强化了 DIA 对不同地区、种族以及组织的情报收集与分析能力。

（2）AI 与军工设备的有机结合。智能军事设备一直是美国军方追求的军事力量发展方向。从技术需求看，AI 分析能力与各类设备传感器数据的集合，成为其需求的一大重点，在 18 个方向中，有 5 个方向涉及相关内容。AI 技术除了能提高设备的性能外，还能实时为所处战区提供包括危险预警、战略分析以及军事策略选择等情报信息支撑。这种支撑甚至可以覆盖到单个士兵等基本作战单元。

（3）快速战区情报生成、分析与处理能力。DIA 与 CIA 在 AI 技术需求的一大不同点在于，DIA 更为着重能在短时间内得到 AI 技术的分析处理结果，压缩情报数据提取、分析到应用所需要的时间。在 18 个方向中，DIA 对大部分方向都要求技术必须具有短时间内快速分析能力，特别是第二大方向就是利用 AI 技术压缩军事情报生成、处理的时间，从而满足实时变化的战场需要。

2.2　美国国家情报机构 AI 技术发展趋势分析

2.2.1　AI 技术将逐步代替大量人工情报工作　随着情报越来越以大数据的形式展现，传统的人工情报采集、分析等工作已经难以适合当前的情报发展趋势。以卫星数据为例，随着卫星的发展和情报收集技术的进步，可收集到的数据正以成倍的速度在增长。美国地理空间情报局的局长 Robert Cardillo 表示，未来 20 年的商用卫星影像情报分析工作，如果需要人来进行的话，将需要近 800 万名图像分析师，目前美国地理空间情报局正积极引入 AI 技术，计划未来该局 75% 情报分析任务将全部自动化，从而提高效率[9]。

2.2.2　社交媒体大数据情报分析得到高度重视　美国《人工智能与国家安全》报告指出，对于社交媒体的数据监测、分析以及筛选是美国国家安全的重要保障之一。AI 技术的引入将成为美国应对海量社交媒体数据的关键工具。从近两年 CIA 支持的 AI 技术项目看，相当一部分是对社交媒体大数据的处理与分析，包括自然语言处理识别技术、图像与情感识别技术等。CIA 肯特学校教情报分析的校长 Joseph Gartin 表示，未来 AI 技术的引入将大大提高 CIA 收集社交媒体数据的规模和速度[9]。

2.2.3　IQT 公司化运作模式正逐渐受到认可　IQT 公司在 1999 年创建，公司的任务是鉴定和投资于维护美国国土安全利益的尖端科技公司，将可以提供出众能力的技术交付给 CIA、DIA、NGA（国家地理空间情报局），以及更广泛的情报界（the larger intelligence community）。目前，IQT 大约 75% 的投资交易都服务于包括 CIA 在内的美国情报界多个机构。美国绝大部分风险投资资金和风险投资公司都是民间的，但 IQT 投资公司的成立打破了这种局面，美国中央情报局作为政

黄敏聪. 美国国家情报体系人工智能技术发展现状分析[J]. 图书情报工作,2018,62(11):127－134.

府的一个机构,每个财政年度为 IQT 提供至少 3500 万美元的资金,而 IQT 则以风险投资的形式为 CIA 培育、传输先进的、可以为其所用的信息技术[10]。近年来,IQT 公司大量投资 AI 技术项目,其占比逐年提高。CIA 目前支持的 137 个 AI 技术情报项目大部分都是通过 IQT 公司筛选并支持。IQT 公司是非营利性质的,除了通过 CIA 经费支持外,主要依托美国各类社会主体的捐赠。这种公司化市场运作模式,极大地加速了美国小型 AI 技术情报企业的发展速度与效率。

2.2.4 庞大的资金支持 据统计,CIA、DIA 以及美国其他国家情报体系机构每年都投入超过 5000 万美元的资金用于支持 AI 技术情报项目(包括 CIA 对 IQT 公司的 3500 万美元支持,IQT 公司不对外透露每个企业的投资额)。此外,通过美国企业、高校以及其他科研基金支持的 AI 技术情报项目金额则更为庞大。在美国《人工智能与国家安全》报告中也表示,"DARPA、IARPA、海军研究办公室和国家科学基金会等机构应增加与 AI 相关的情报技术基础研究经费,向美国 IQT 公司提供更多资源,促进国家安全机构和 AI 商业公司的合作"[1]。由此可见,未来美国对于国家情报体系中 AI 技术项目的投入将会越来越多。

此外,在社会层面,截至 2017 年 7 月,美国 AI 初创企业的融资金额已经高达 978 亿元,占全球总融资额的 50.1%(中国 635 亿元,占全球 33.18%,见图 1),这样庞大的社会资金投入给 AI 初创企业提供了良好的金融支撑,而美国国家情报体系也从中受益,推动了美国国家情报体系 AI 技术应用的发展[11]。

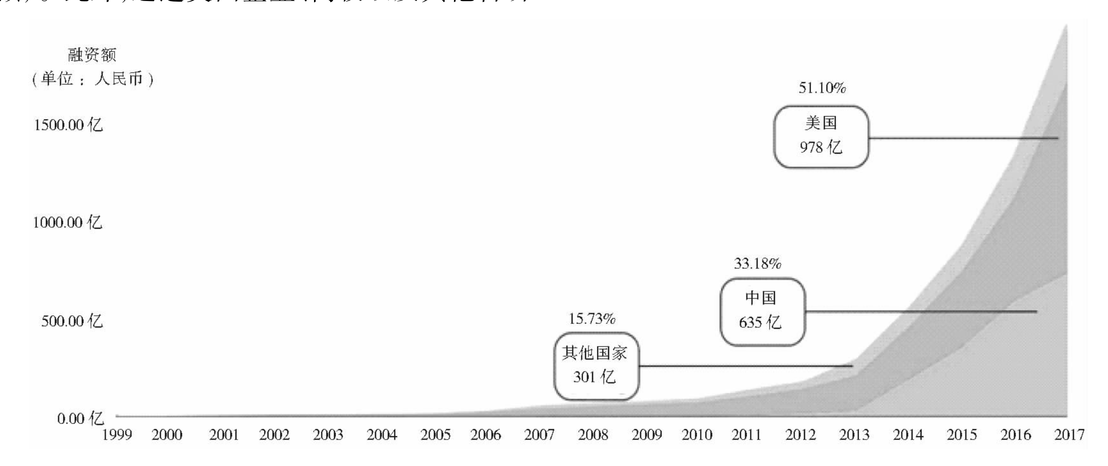


图 1 中美 AI 产业累计融资额对比(单位:人民币)[11]

2.2.5 硅谷正成为美国国家情报体系 AI 技术的重要创新源 从 IQT 公司支持的项目以及其他国家情报机构发布的信息看,超过 80% 的 AI 技术情报项目承担企业主要集中在硅谷地区。这一方面是由于硅谷集聚了大量的 AI 技术人才储备,另一方面是由于其发达的风险投资基金。这种集聚效应促进了 AI 技术情报项目的协同合作,并涌现了大量的创新应用。IQT 公司以及美国其他国家情报体系都相继在硅谷地区建立了分支机构,从而快速识别企业以及项目。综上所述,硅谷正成为美国国家情报体系 AI 技术的重要创新源。

2.2.6 "反 AI"技术进攻与防御能力 美国《人工智能与国家安全》报告中表示,随着 AI 技术的深入发展,美国国家情报体系应大力投资"反 AI"的进攻和防御能力。目前,已有研究表明,一些 AI 技术可以被利用来进行对情报的伪装,例如利用 AI 技术在社交媒体散播谣言,鼓动社会活动,或者利用 AI 技术制造虚假的社会与商业数据,从而使 AI 情报分析结果有错误。这种 AI 技术的应用甚至可以影响到国家决策。因此,反"AI"技术成为了美国国家情报体系未来重要的关注方向。

2.2.7 云端应用逐渐成为 AI 情报项目的重要依托载体 2016 年－2017 年,CIA 已经支持了 3 个创新项目用于将 AI 技术情报项目部署在亚马逊等云端平台。利用云平台的特性,进一步加快 AI 技术情报项目的数据收集广度、深度以及互联互通能力。此外,为了应对云平台应用而引发的安全问题,CIA 也支持对于 AI 技术情报项目威胁检测能力的项目,从而确保国家情报体系的安全性。

2.2.8 美国政府谨慎应对 AI 情报分析结果 目前,美国政府对于 AI 技术情报分析结果的态度显得有些过于保守。CIA 等机构表示,AI 技术情报分析结果在提交给国家决策者参考之前,首先要保证人类自己可以搞懂这中间的推演过程。说服政府高层(包括美国总统)取信于这些在他们看来是由"机器人"生成的情

报报告是今后 AI 技术情报项目开发者所面临的一大挑战[9]。

3 美国国家情报体系 AI 发展的优势分析

3.1 众多的初创企业支撑

从 CIA、DIA 等政府机构支持的 AI 技术项目看,超过 50% 的项目由初创企业承担,而且主要集中在硅谷。截至 2017 年 6 月,全球 AI 初创企业总数达到 2 542家,其中美国拥有 1 078 家(42%);中国其次,拥有 592 家(23%);其余 872 家分布在瑞典、新加坡、日本、英国、澳大利亚、以色列、印度等国家。同时,美国 AI 初创企业从 1991 年开始出现,而中国则到 1996 年才出现。这样庞大的 AI 初创企业规模支撑了美国国家情报体系 AI 技术的快速发展[11]。

3.2 国际事务的主导地位激发了美国国家情报体系 AI 技术的需求

美国作为世界强国,几乎参与全球大部分国际事务,在不同国家与地区均有国家情报需求,面对日益繁杂的国际形势,其对于 AI 技术的需求越发强烈。在美国 AI 初创企业中,排名前 3 的领域为自然语言处理(252 家)、机器学习应用(242 家)以及计算机视觉与图像(190 家)。这与美国 CIA 以及 DIA 的需求高度一致,面对各国各地区的语言不同情况,CIA 以及 DIA 都将自然语言处理列为重要支持类别,而机器学习应用以及计算机视觉等两个领域则得到了相关军事情报机构(包括 DIA)的大力支持。与美国情况不同,中国 AI 初创企业的领域主要面向产业制造领域,例如智能机器人等[11]。

3.3 AI 技术人才供给充足确保了美国国家情报体系 AI 技术的快速发展

美国 1 078 家 AI 初创企业约有 78 700 名员工,中国 592 家企业约有 39 200 名员工,只有美国的 50%。此外,美国在 5 大 AI 技术热点领域人才数量均全面领先。自然语言处理领域,美国 20 200 人,中国 6 600 人,美国技术人数是中国的 3 倍;处理器/芯片领域,美国 17 900 人,中国 1 300 人,美国员工人数是中国的 13.8 倍;机器学习应用领域,美国 17 600 人,中国9 800 人,美国员工人数是中国的 1.8 倍;智能无人机领域,美国 9 220 人,中国 4 660 人,美国员工人数是中国的 1.98 倍;计算机视觉与图像领域,美国 4 335 人,中国 1 510人,美国员工人数是中国的 2.87 倍。CIA 肯特学校教情报分析的校长 G. Joseph 表示,美国高素质 AI 技术人才储备是 CIA 未来 AI 技术项目发展的关键基础与重要因素[11]。

4 美国国家情报体系 AI 技术发展现状对我国的启示

4.1 我国国家情报体系 AI 技术应用现状

在国家层面,“人工智能”一词于 2016 年 3 月被写入国家“十三五”规划纲要。2017 年 7 月,国务院关于印发《新一代人工智能发展规划的通知》,从国家层面对人工智能进行系统布局,推进主体落实在科技部。包昌火等专家认为,目前我国国家情报体系尚未完全建立,主要推动方主要集中在国防部、国家安全部以及公安部。根据公开信息以及文献调研看,我国国家情报体系对于 AI 技术的大规模研究、开发与应用始于 2014 年,例如中国兵器工业集团与中国人工智能学会联合推动建立“中国无人系统院士专家工作站”[12],云从科技公司与公安部联合构建“人脸识别产业化及应用项目”[13]等。虽然我国国家情报机构近年来都相继开展了 AI 技术应用的探索,但是与美国国家情报机构相比还存在以下不足之处:

4.1.1 *没有完全引导* 我国企业 AI 技术资源服务国家情报体系从美国的情况看,依托 IQT 公司,美国国家情报机构与企业界,特别是硅谷地区企业建立了紧密联系,使得国家情报机构的需求能快速满足,而大量 AI 初创企业也能得到大量资金资助。中国作为目前全球仅次于美国的 AI 产业大国,AI 技术资源(企业、技术、人才、设备、平台)丰富,而我国目前尚没有一套完善的体制机制以及平台能充分引导这些 AI 技术资源服务我国国家情报机构。这一方面是由于体制机制的限制,另一方是由于传统保密观念的制约,诸多国家情报机构宁愿将技术需求项目交由下属研究院所来完成。

4.1.2 *缺乏推动* AI 技术应用主要承担方美国国家情报机构的 AI 技术应用与推广主要有 CIA 负责,这一方面能极大减少重复性投入,而且也方便各个机构之间的数据统一、协调与处理。目前,CIA 已经在利用云端平台,建立美国国家情报机构之间的 AI 技术云端应用平台。而在我国,尚未有一家独立机构能承担相关 AI 技术的应用与推广工作,这使得大部分 AI 技术项目都存在重复投入现象,例如,国防部与公安部都有类似的 AI 智能人脸识别系统在开发。这种现象的存在还阻碍了各个国家情报机构之间建立协同合作机制与平台。

4.2 美国国家情报体系 AI 技术发展现状对我国的启示

4.2.1 将国家情报体系 AI 技术应用项目向全社会企业开放 从美国的经验看,In-Q-Tel 公司的市场化运作模式是美国国家情报体系 AI 技术应用快速发展的重要助推剂,大量美国 AI 初创企业得到政府项目支撑,这些企业无论从运行效率还是技术迭代程度都比传统科研院所或者政府下属研究机构要高。在我国国家情报体系的构建中,往往存在一种保守主义,并认为将国家情报体系的项目交由私人中小型初创企业承担是不可靠的,一方面是担心中小型初创企业不具备能力,另一方面是认为又存在泄密的风险。从公开的信息看,我国情报机构大部分类似的项目还是主要依托机构下属科研院所、高校或大型信息企业。这样保守的态度,一方面不利于国家情报体系的技术快速应用升级,另一方面也不利于培育 AI 技术市场。因此,我国应以美国 In-Q-Tel 公司为模板,成立由政府经费为主要支持的类似国家技术情报技术市场培育公司,通过对我国 AI 技术初创企业的支持,为国家情报机构提供可靠的 AI 技术的市场化解决方案。

4.2.2 注重"反 AI"技术进攻与防御能力的培育 在全球大多数国家刚开始注重对 AI 技术运用时,美国国家情报机构已经开始着手如何进行"反 AI"技术进攻与防御能力的培育。在《人工智能与国家安全报告》中,该项能力被列为美国在未来国家情报体系构建中领先全球的关键基础能力。"反 AI"技术进攻与防御能力的培育除了能在传统国家情报领域发挥作用外,其在军事层面的作用也越来越大。目前,美国 DIA 已经在战场层面开展了类似区域战争 AI 技术应用场景的项目(见表 2)。因此,我国更应加快"反 AI"技术进攻与防御能力的培育工作。

4.2.3 加大对国家情报体系 AI 技术人才以及科研机构的培育力度 从表 3 可见,目前 AI 技术领域前 20 的学校中,我国只有北京大学(排名 12)、清华大学(排名 16)以及香港科技大学(排名 17)进入排名,而美国无论从高校数量、顶级学者数量以及重要论文数量都占据绝对领先地位[14]。大量具有国际竞争力的科研机构以及学者是美国 AI 技术得以领先全球的关键,也是美国国家情报体系 AI 技术创新的根本性支撑。除了一般的科研机构外,近年来美国 CIA 也在其下属的培训机构——肯特学院,陆续开展了 AI 技术人才培训以及相关课程,依托美国大量的 AI 创新资源,使得肯特学院的 AI 技术人才培育取得了良好的效果。目前,我国互联网企业发达,百度、阿里巴巴以及腾讯三大互联网企业也陆续开展了 AI 技术的探索,因此,我国应该借助互联网企业的 AI 创新资源,通过政府以及科研机构的合作,建立我国国家情报体系的 AI 技术人才培育体系。

表 3 AI 领域前 20 高校及其学者数量[14]

序号	学校名称	国家	顶级学者数量	顶级会议论文数量
1	卡耐基梅隆大学	美国	111	638
2	加州大学伯克利分校	美国	48	285.1
3	华盛顿大学	美国	45	262.5
4	麻省理工学院	美国	48	235.2
5	斯坦福大学	美国	40	226.9
6	康奈尔大学	美国	46	212.8
7	佐治亚理工学院	美国	53	208.5
8	宾夕法尼亚大学	美国	29	184.4
9	多伦多大学	加拿大	39	164.1
10	伊利诺伊大学香槟分校	美国	44	161.6
11	南加州大学	美国	32	161.3
12	北京大学	中国	69	154.9
13	爱丁堡大学	英国	47	151.2
14	东京大学	日本	40	145.2
15	密歇根大学	美国	32	135.2
16	清华大学	中国	45	132.1
17	香港科技大学	中国	29	126.1
18	马萨诸塞大学阿默斯特分校	美国	36	122.4
19	马里兰大学	美国	26	112.6
20	新加坡国立大学	新加坡	33	102.3

说明:数据截至 2017 年 7 月

4.2.4 注重 AI 技术项目在云端平台的运用与保护 从 CIA 部署的 137 个 AI 情报项目看,CIA 已经有计划将美国国家情报体系逐步在云端平台进行部署,包括部署在亚马逊或者微软云平台。同时,CIA 等机构也同步开展了针对 AI 情报项目的网络威胁与保护。CIA 预期,随着情报数据量级的飞跃式发展,依托传统信息化平台已经难以满足情报需求,特别是 AI 情报项目的对数据收集的广度以及深度,目前只有云端平台能满足未来 AI 技术需求。同时,依托云端平台,政府许可的任何人都可以在任何时候任何地方利用美国国家情报体系的强大 AI 资源。例如,美国军方已经有计划实施战区危险预警情报项目,美国军人可以依托移动设备快速接入云端平台,快速了解当前战区的实时威胁,并可通过脸部识别等手段,快速了解所见的每一个人的威胁程度等。类似的云端 AI 情报项目支撑美国全球国际事务的参与。基于此,我国国家情报体系 AI

情报项目应加快其在云端平台的运用实践,并探索利用我国互联网企业的强大云端支撑能力,提高项目的运用效率以及保护力度。

参考文献:

[1] Artificial intelligence and national security[R/OL]. [2017-12-08]. https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf.
[2] 包昌火,马德辉,李艳,等. 我国国家情报工作的挑战、机遇和应对[J]. 情报杂志,2016,35(10):1-6,17.
[3] 张家年,马费成. 我国国家安全情报体系构建及运作[J]. 情报理论与实践,2015,38(8):5-10.
[4] 美国中情局对 AI 有多重视? 137 个项目同时推进! [EB/OL]. [2017-12-08]. https://wallstreetcn.com/articles/3029612.
[5] IQT-portfolio [EB/OL]. [2017-12-08]. https://www.iqt.org/portfolio/.
[6] DIA innovation implementation plan [R/OL]. [2017-12-08]. http://www.dia.mil/Portals/27/Documents/Business/Innovation/2015_2016_DIA_INO_Implentation_Plan_RD.pdf.
[7] 美国情报部门用人工智能当间谍[EB/OL]. [2017-12-08]. https://www.leiphone.com/news/201708/LUzMRHM7YeuzxmBi.html.
[8] Needipedia[EB/OL]. [2017-12-08]. http://www.dia.mil/Business/Needipedia/.
[9] 美国中央情报局(CIA)如何使用人工智能收集社交媒体数据[EB/OL]. [2017-12-08]. http://www.4hou.com/info/news/7629.html.
[10] 揭秘 In-Q-Tel:中情局神秘投资机构的传奇[EB/OL]. [2017-01-08]. http://baijiahao.baidu.com/s?id=1585816676680699324&wfr=spider&for=pc.
[11] 中美两国人工智能产业发展全面解读[R/OL]. [2017-12-08]. http://www.tisi.org/Public/Uploads/file/20170802/20170802172414_51007.pdf.
[12] 我国成立无人系统院士专家工作站推动智能系统转型[EB/OL]. [2017-01-08]. http://scitech.people.com.cn/n/2014/0617/c1057-25157153.html.
[13] 云从科技入选国家发改委人工智能重大工程[EB/OL]. [2017-01-08]. http://tech.sina.com.cn/roll/2018-01-07/doc-ifyqinzs9671254.shtml.
[14] 2017 全球人工智能人才白皮书[R/OL]. [2017-12-08]. http://www.tisi.org/Public/Uploads/file/20171201/20171201151555_24517.pdf.

An Analysis of the Development of Artificial Intelligence in the United States Intelligence Community

Huang Mincong
Guangdong Science and Technology Library (Guangdong Institute of Scientific & Technical Information and Development Strategy), Guangzhou 510070

Abstract: [**Purpose/significance**] This paper analyses the background and significance of the application of AI in the United States Intelligence Community (USIC) and summarizes the developmental trends of AI in the USIC based on contents, directions and models of application by the national intelligence organizations such as the Central Intelligence Agency (CIA) and Defense Intelligence Agency (DIA). According to the above analysis, this paper proposes the implication for the application of AI by the Chinese intelligence agencies. [**Method/process**] This paper uses the methods of literature review and comparative analysis. Firstly, it analyzes the application contents of the AI projects in organizations such as the CIA and the DIA. Secondly, it analyzes the cutting edges of AI technology in the USIC. [**Result/conclusion**] The USIC has been embracing the AI technology in an unimaginable way in terms of the number of projects, funding capital, and developmental plans, especially with the promotion of In-Q-Tel company as the key factor. The intelligence agencies in China should draw on the advanced experiences from the USA, advance the application of AI technology and pay special attention to cooperating with the Chinese Internet companies.

Keywords: US United States Intelligence Community AI